Encrypted Traffic Analysis (ETA) : détection de menaces dans le trafic chiffré

Lien : https://innov-systems.com/formation/encrypted-traffic-analysis-eta-detection-de-menaces-dans-le-trafic-chiffre

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**RT64**	**Sécurité Du Réseau**

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principes de l’analyse du trafic chiffré
- Maîtriser les techniques d’Encrypted Traffic Analysis (ETA)
- Exploiter les métadonnées réseau pour détecter les menaces
- Appliquer le machine learning à la cybersécurité réseau
- Identifier les attaques dissimulées dans le trafic TLS/HTTPS
- Intégrer ETA dans un SOC moderne
- Utiliser les outils d’analyse réseau spécialisés
- Réduire les angles morts liés au chiffrement
- Améliorer la détection des menaces avancées (APT)
- Concevoir des systèmes de détection comportementale
- Étudier des cas concrets d’attaques sur trafic chiffré
- Développer des compétences en cybersécurité avancée réseau

POUR QUI ?

- Analystes SOC
- Ingénieurs cybersécurité
- Data scientists sécurité
- Network security engineers
- SOC managers
- Consultants cybersécurité
- Architectes sécurité réseau
- Threat intelligence analysts
- Administrateurs réseau
- Experts NDR (Network Detection and Response)
- Toute personne impliquée dans la détection des menaces réseau

Innov Systems

Programme détaillé

1 / Introduction à l’Encrypted Traffic Analysis (ETA)

- Définition et enjeux de l’analyse du trafic chiffré
- Évolution des communications chiffrées (TLS, HTTPS, QUIC)
- Défis pour la cybersécurité moderne

2 / Fondements du trafic réseau chiffré

- Protocoles de chiffrement réseau (TLS 1.2/1.3)
- Métadonnées exploitables malgré le chiffrement
- Limites de l’inspection classique (DPI)

3 / Techniques d’analyse du trafic chiffré

- Analyse statistique des flux réseau
- Fingerprinting des connexions
- Analyse comportementale des sessions

4 / Machine Learning appliqué à l’ETA

- Classification des flux malveillants
- Détection d’anomalies réseau
- Feature engineering sur métadonnées réseau

5 / Détection de menaces avancées

- C2 (Command & Control) dissimulés
- Exfiltration de données chiffrées
- Malware utilisant TLS/HTTPS

Innov Systems

6 / Outils et frameworks d’analyse ETA

- Zeek (Bro), Wireshark et Suricata
- Solutions SIEM et NDR
- Intégration avec pipelines de sécurité

7 / Architecture de détection en environnement réel

- Collecte de logs réseau à grande échelle
- Traitement en temps réel des flux
- Intégration dans SOC (Security Operations Center)

8 / Limitations et contournements

- Faux positifs et faux négatifs
- Techniques d’évasion des attaquants
- Limites du machine learning en ETA

9 / Cas d’usage et scénarios industriels

- Détection de ransomware via trafic chiffré
- Surveillance des environnements cloud
- Sécurité des réseaux d’entreprise hybrides

10 / Études de cas et mise en pratique

- Analyse de trafic chiffré réel
- Construction d’un modèle de détection ETA
- Bonnes pratiques en SOC

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

22 au 26 Fév. 2027	Présentiel - Casablanca
19 au 23 Avr. 2027	Présentiel - Casablanca
14 au 18 Juin 2027	Présentiel - Casablanca
09 au 13 Août 2027	Présentiel - Casablanca
04 au 08 Oct. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés